Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

7 August 2015

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
richard.t.willis@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance:	7 February 2014 – 7 February 2016
Total Contract Amount:	$475,359 (Base)
Amount of Incremental Funds:	$440,469
Total Amount Expended (thru fiscal July):	$325,413

Attention: Dr. Richard Willis
Subject: Quarterly Progress Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 AUG 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **BBN Technologies,,10 Moulton Street,,Cambridge,,MA,02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**13**	

SEAKEY Quarterly Progress Report for the
Period 26 April 2015 – 4 August 2015 (100 Days)

Section A. Project Schedule

The Year 2 timeline below identifies the high level SeaKey tasks and their durations.

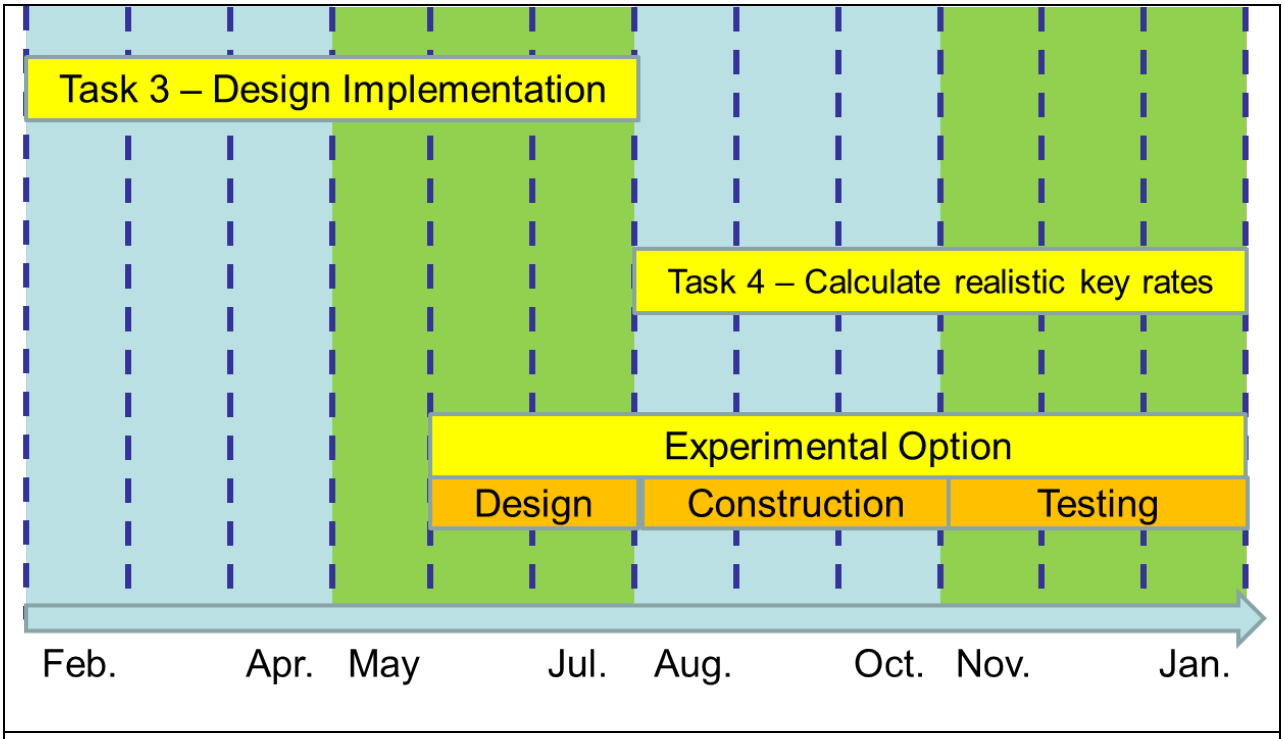

Figure 1: SeaKey year 2 program schedule.

Section B. Technical Progress

SUMMARY

In this report we summarize the technical progress accomplished during the first quarter of the second year of the SeaKey program. Our progress stems from our year 1 work on the program executing tasks 1 and 2. The two major tasks we are executing this year, identified in figure 1, are: (1) designing a proposed implementation for a free-space QKD link optimized for operation in a naval environment and (2) calculating the achievable key rate of the aforementioned QKD link in realistic environmental conditions.

This quarter we have evaluated literature which calculates key rates of CV QKD systems, primarily as a function of realistic receiver parameters. Subsequently, we have constructed our own models for CV QKD rate calculations, awaiting parameterization from experimental results from our own laboratory, or from guidance from ONR. This report contains a technical memo from Boulat Bash describing the details of the homodyne receiver model under construction.

In an effort to meet the aggressive key rates required by ONR for the QKD system under study our team continues to evaluate limits of multi-spatial QKD systems, using multiple Gaussian beams to provide a linear increase to the key rates achievable in free-space, when rates for a single mode are limited by loss and noise. This report also contains a technical memo from Boulat Bash describing the details of the multi-mode analysis being performed in collaboration with Jeff Shapiro at MIT.

TECHNICAL RESULTS

Modeling Gaussian-modulated coherent-state quantum key distribution using balanced homodyne detector

Introduction

The rate of quantum key distribution (QKD) critically depends on the loss and noise in the system. The range of continuous-variable (CV) QKD systems is especially sensitive to excess noise in the system. Here we analyze the performance of the CV Gaussian-modulated coherent state QKD protocol that uses a practical balanced homodyne detector (BHD). We build on the work in [Chi *et al.*] by

- accurately modeling the atmospheric absorption and scattering,
- optimizing the modulation power,
- optimizing the laser repetition rate, and
- analyzing the impact of the collective attacks on the QKD rate.

We also rely on the formulae and references presented in [Scarani *et al.*].

QKD system performance model

The QKD rate in bits per second of any QKD system is expressed as follows:

$$r=\max(0,\beta I_{AB}-I_{BE})\times R \qquad (1)$$

where I_{AB} measures the shared mutual information between Alice and Bob and I_{BE} measures the same between Bob and Eve. In practice, the effective amount of information shared between Alice and Bob is reduced by error correction and reconciliation, which is captured by factor $\beta \leq 1$. Furthermore, I_{AB} and I_{BE} quantify the shared information in bits per pulse. We thus multiply by the laser repetition rate R in pulses per second to obtain the QKD rate in bits per second.

The information measures I_{AB} and I_{BE} depend on, respectively, Alice/Bob and Eve capabilities. Here we assume that Alice and Bob use Gaussian-modulated laser light source over a free-space optical channel with a balanced homodyne receiver. Thus, the expression for I_{AB} is a familiar Shannon capacity of a classical additive white Gaussian noise (AWGN) channel:

$$I_{AB}=\frac{1}{2}\log_2\left[1+\frac{V_A}{1+\delta}\right], \qquad (2)$$

where V_A is the Gaussian modulation power in photons per pulse and δ is the noise in photons per pulse measured at the input (thus, noise originating at various locations along the system is scaled according to the gain/loss of the channel up to that point). Noise δ is expressed as follows:

$$\delta=\frac{1-\eta G}{\eta G}+\delta_A+\delta_V+\frac{\delta_{LO}+\delta_e}{\eta G}, \qquad (3)$$

where $\frac{1-\eta G}{\eta G}$ is the loss-induced vacuum noise, δ_A is noise from the imperfections outside Bob's system, δ_V is noise introduced by the electrical pulse overlap because of the finite response time of the BHD, δ_{LO} is the noise associated with local oscillator (LO) fluctuations in the presence of incomplete subtraction of a BHD, and δ_e is the electronic noise at Bob's homodyne detector.

We consider two types of attacks on Alice and Bob's system by Eve. First, we analyze the *individual* attack, where Eve attacks each of the quantum systems transmitted by Alice to Bob independently of the others, and measures her ancillas before classical post-processing. In this case, the information Eve obtains is classical, and I_{EB} is expressed as follows [Lodewyck *et al.*, 2005]:

$$I_{BE}=\frac{1}{2}\log_2\left[\frac{1+\eta G(V_A+\delta_A+\delta_V)+\delta_{LO}+\delta_e}{\eta/(1+G(\delta_A+\delta_V+(V_A+1)^{-1}-1)+\delta_{LO}/\eta)+1-\eta+\delta_e}\right]. \quad (4)$$

This model assumes that Eve controls all noise sources *except* the electronic noise at Bob's detector δ_e.

The collective attack assumes that Eve attacks each of the quantum systems transmitted by Alice to Bob independently of the others but can keep her ancillas in a quantum memory for any amount of time. Thus, Eve potentially has access to all the classical information encoded in the quantum states that she collects. This is measured using the quantum generalization of the classical Shannon mutual information, known as *Holevo* information, and is expressed as follows [Scarani *et al.*, Section V.B.5]:

$$I_{BE}=\chi(B:E)=\tilde{g}(\lambda_1)+\tilde{g}(\lambda_2)-\tilde{g}(\lambda_3), \quad (5)$$

where $g(x)=(x+1)\log_2(x+1)-x\log_2 x$ is the entropy of a thermal state with mean photon number x and $\tilde{\lambda}_k=\frac{\lambda_k-1}{2}$ with

$$\lambda_{1,2}^2=\frac{1}{2}\left(A\pm\sqrt{A^2-4B}\right) \quad (6)$$

$$\lambda_3^2=\frac{1+V_A+(1+V_A)^2\delta}{1+V_A+\delta} \quad (7)$$

and

$$A=(1+V_A)^2(1-2\eta G)+2\eta G+[\eta G(1+V_A+\delta)]^2 \quad (8)$$

$$B=[\eta G(1+\delta+V_A\delta]^2. \quad (9)$$

Here it is assumed that Eve controls *all* noise sources. We note that collective attack is optimal for Eve: that is, (5) is the maximum amount of information that Eve can access in a CV QKD system [Renner and Cirac].

It is clear that the QKD rate given in (1) is a complicated function of the modulation power V_A; we must thus find the optimal value of V_A that maximizes the QKD rate. It turns out that the repetition rate R must also be optimized, as the improvement in bits-per-second QKD rate comes at the cost of increased noise from the pulse overlap. We describe the models of noise and loss, and provide the parameters we use in our calculations next.

Noise and loss models

Channel, detector, and coding efficiency

We operate at the standard λ=1.55μm wavelength. In our calculations we use the formulae for propagation of a normalized focused beam in free space without accounting for the effects of turbulence (analysis of the impact of turbulence is on our research agenda in Section V). However, we model the atmospheric absorption and scattering using MODTRAN [Berk *et al.*]. Thus, channel efficiency is expressed as follows:

$$G=G_T\times\exp[-\alpha L], \qquad (10)$$

where $\exp[-\alpha L]$ is the attenuation from atmospheric absorption and scattering, and G_T is the power transmissivity of a channel induced by transmitting a normalized focused beam in vacuum from a circular aperture of radius r_T to a circular aperture of radius r_R located L meters away. We assume $r_T=r_T=0.1$ m. The wavelength-dependent extinction coefficient $\alpha=0.917$ is drawn from MODTRAN "Mid-Latitude Summer (MLS)" atmospheric model at a 10 m elevation from the ground level with 23 km visibility in clear weather. We obtain G_T by evaluating [Shapiro, (18)] with turbulence strength $C_n^2=0$:

$$G_T\text{Error!} \qquad (11)$$

where $J_n(x)$ is the n-th order Bessel function of the first kind, and $D_f^0=\left(\frac{\pi r_R r_T}{4\lambda L}\right)^2$ is the Fresnel number product. Our error correction and reconciliation coding efficiency is $\beta=0.898$, corresponding to the results from experimental systems [Lodewyck *et al.*, 2007]. We use detector efficiency $\eta=0.84$ in the calculations that follow.

Noise models

We set the electronic noise and the noise from the imperfections outside Bob's system to $\delta_e=0.045$ and $\delta_A=0.056$ photons per pulse, respectively, as is done in [Chi *et al.*].

Per eq. (8) in [Chi *et al.*], the excess noise contributed by the pulse overlap is:

$$\delta_V=2(V_A+1)\times\exp[-B^2/R^2], \qquad (12)$$

where B is the bandwidth of the detector and R is the laser repetition rate. We set the bandwidth of the detector to B=100 MHz. Eqs. (1) and (12) present a trade-off: increasing R increases QKD rate in bits per second, but also increases the noise from pulse overlap. Therefore, we optimize R, along with V_A, to achieve the maximum QKD rate.

The noise from the fluctuations of the local oscillator (LO) is given by [Chi *et al.*, (11)]:

$$\delta_{LO}=\frac{\langle \Delta I_{LO}^2 \rangle \kappa}{I_{LO}}, \quad (13)$$

where I_{LO} is the number of photons in the LO pulse, $\langle \Delta I_{LO}^2 \rangle$ is its variance, and κ is the total imbalance of the detector. Denote by $\{t_1,t_2\}$ the beam splitter transmission and reflection coefficients and by $\{G_1,G_2\}$ the amplifier gains associated with two photodiodes. Assuming $t_1^2 \approx t_2^2$ and $G_1 \approx G_2$, $\kappa \approx \kappa_{opt}+\kappa_{el}$, where $\kappa_{opt}=t_1^2-t_2^2$ and $\kappa_{el}=\frac{G_1-G_2}{G_1+G_2}$. In the calculations that follow we discuss the impact of δ_{LO} in terms of generalized common-mode rejection ratio (CMRR) which is measured in decibels and defined by [Chi *et al.*, (12)]:

$$CMRR=-20\log_{10}(2\delta). \quad (14)$$

We calculate δ_{LO} for an LO with power 20 mW and power stability 0.1 %RMS.

Results

The QKD rate optimized over modulation power V_A and repetition rate R is presented in Figure 2. We also plot the optimal values of V_A and R in Figures 3 and 4, respectively.

Clearly, only guaranteeing security against the less sophisticated individual attacks allows greater rate. Also notable is the large CMRR (and, correspondingly, small κ) required to attain positive QKD rate at longer transmission ranges. We note that increasing the detector efficiency η and the error correction/reconciliation efficiency β would substantially improve the QKD rate.

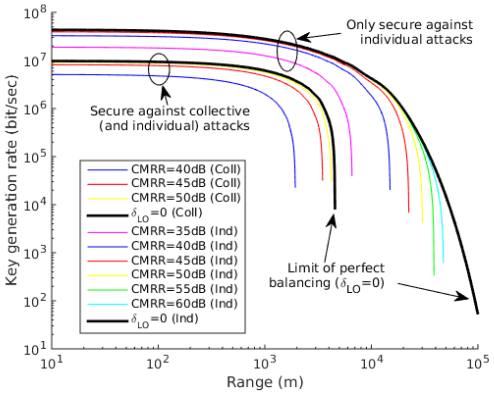

Figure 2: QKD rate optimized over modulation power V_A and repetition rate R.

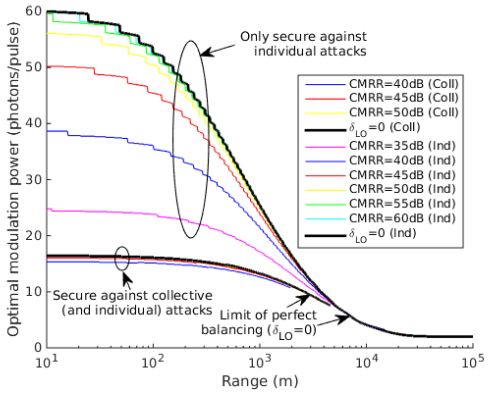

Figure 3: Optimal modulation power V_A.

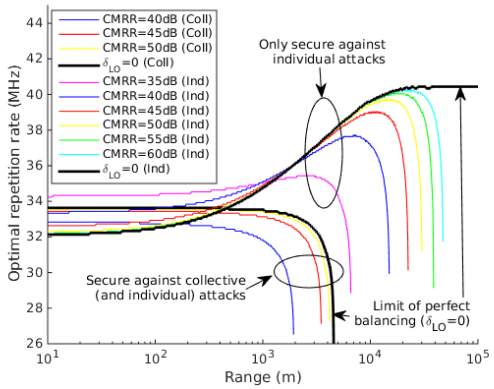

Figure 4: Optimal repetition rate R.

References

[Chi *et al.*] Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A I Lvovsky, and Liang Tian, A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution," New Journal of Physics **13**, 013003 (2011).

[Scarani *et al.*] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301-1350 (2009).

[Lodewyck *et al.*, 2005] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**, 050303 (2005).

[Renner and Cirac] R. Renner and J. I. Cirac, de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).

[Berk *et al.*] Alexander Berk, Gail P. Anderson, Prabhat K. Acharya, Lawrence S. Bernstein, Leon Muratov, Jamine Lee, Marsha Fox, Steve M. Adler-Golden, James H. Chetwynd, Jr., Michael L. Hoke, Ronald B. Lockwood, James A. Gardner, Thomas W. Cooley, Christoph C. Borel, Paul E. Lewis, and Eric P. Shettle, MODTRAN5: 2006 update," (2006) pp. 62331F-62331F-8.

[Shapiro] Jeffrey H. Shapiro, Near-field turbulence effects on quantum-key distribution," Phys. Rev. A **67**, 022309 (2003).

[Lodewyck *et al.*, 2007] Jérôme Lodewyck, Matthieu Bloch, Ra_ul Garc__a-Patr_on, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier, \Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).

Quantum key distribution using multiple Gaussian focused beams

Recent proliferation of suggestions on using OAM modes for QKD begs a question of whether it is worth it (i.e., how much do we really gain after putting in the effort to generate and separate those orthogonal modes). Here is the list of some recent papers on this:

- http://iopscience.iop.org/1367-2630/17/3/033033/article
- http://www.nature.com/nphoton/journal/v9/n6/full/nphoton.2015.95.html
- http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.113.060503
- http://arxiv.org/pdf/1402.2602.pdf
- http://www.ncbi.nlm.nih.gov/pubmed/22714347
- http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6671930
- http://cpl.iphy.ac.cn/fileup/PDF/201-1422.pdf

We plot some of our recent calculations in Figure 5. This does not include turbulence yet, and is done assuming a discrete-variable (decoy state) BB84 protocol. The yellow curve is a single-spatial-mode baseline that uses one Gaussian laser beam for QKD. The red curve assumes multiple (an optimal number of) focused beams with an optimal choice of the nearest-neighbor overlap between spots at the receiver aperture plane

(the optimal overlap is range dependent), and an optimal size and positioning of the beam waist along the channel length. This calculation assumes a unity-fill factor single-photon detector array with each beam focused at the center of one detector pixel. The blue curve uses orthogonal (HG or LG) modes, assuming those spatial modes can be modulated and separated without loss (which is clearly being very optimistic). The blue curve assumes Gaussian (soft) apertures, and the other two (for the focused beam calculations) assume square apertures of the same area as the soft aperture.

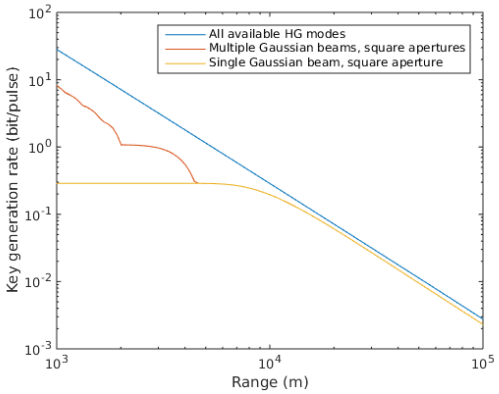

Figure 5: The comparison of the use of the multiple Gaussian laser beams vs. orthogonal modes.

The message from these results seems to be:

1. one can gain a potentially between 1 to 2 orders of magnitude in key rate over a 1 km link by using multiple focused beams, BUT

2. doing QKD using OAM modes is not worth it. The incremental gain by using OAM modes is relatively small (around a factor of 7) and the losses associated with generating/separating these modes is likely to offset this gain.

In fact, the performance of the multiple focussed beam system (the red curve) might improve further if we use hexagonally-packed beam spots as opposed to using a square grid. However, we have not examined that yet.

We are currently working on extending these results to turbulent propagation (with and without adaptive optics). Turbulence will clearly adversely affect all the systems, but it is not clear which one (the multiple focussed beam vs. the multiple HG/LG modes) will be affected more.

NEXT STEPS

In the next quarter we will be specifically evaluating the published noise specifications of balanced photodetector pairs. These values will provide the requirements for LO power at the receiver, as well as help define fundamental limits on the key exchange rate

achievable [1]. Continuing forward we will include non-idealities that were identified in year 1 of the SeaKey program, such as loss and turbulence in the link.

Research agenda

There are several follow-on modeling tasks on our research agenda:

1. Incorporate turbulence into the atmospheric model discussed in Section III+.1667emA. This would substantially improve the applicability of the model to naval communication scenarios;

2. Refine the model for the fluctuations of the LO in Section III+.1667emB, including potential mitigation of such fluctuation by, e.g., attenuating one of the detector arms to improve the balance;

3. Investigate improving QKD rate by using multiple beams for CV QKD;

4. Work with experiments team to measure characteristics of the equipment available in the laboratory and test how well the model matches reality.

Section C. Problem Areas – Identification

There are no anticipated problems or issues to report at this time.

Section D. Financial Update

Financial Chart reflecting Year 2: